Backdoors & Breaches Quick Start

What is it?

- Security incident response game
- Permits you to test your IR capability
- Generate random scenarios to test against
- Players can include:
  - Security team
  - IT
  - HR
  - Legal
  - Entire company

Gameplay overview

- Need to identify
  - How attacker first gained access
  - How they gained a foothold on the network
  - How they are maintaining access
  - Network channel being used for communications
- You only get 10 rounds
  - Need to ID all four attributes above
  - If not, you fail
  - Some scenarios can end more quickly

Do you feel lucky?

- Dice roll identifies success or failure
- Based on D20 dice
  - Can be cheaply purchased
  - There's an app for that!
  - Can cut out and make your own
- When you roll
  - 1-10 = action failed
  - 11-20 = action successful

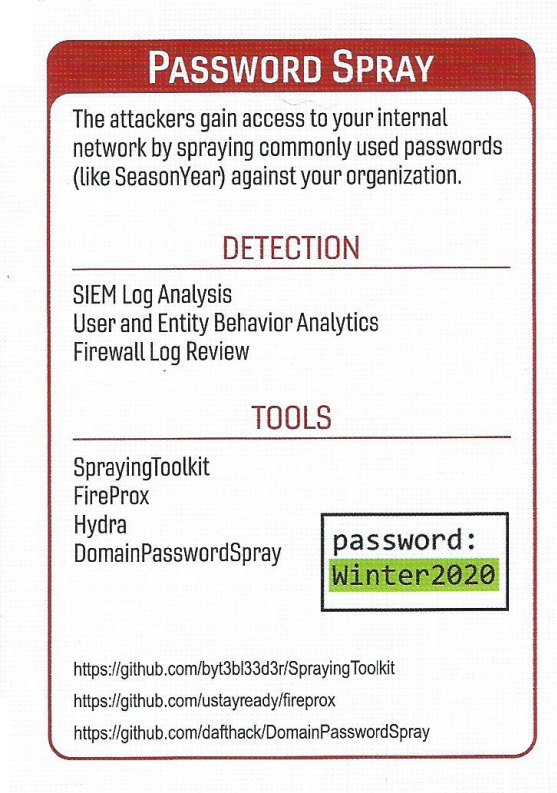
Dice roll modifiers

- If you have a matching procedure card = +3 to rolled value
- When 1 or 20 is rolled, an "inject" card is introduced
- If 3 failed rolls in a row, "inject" card is introduced

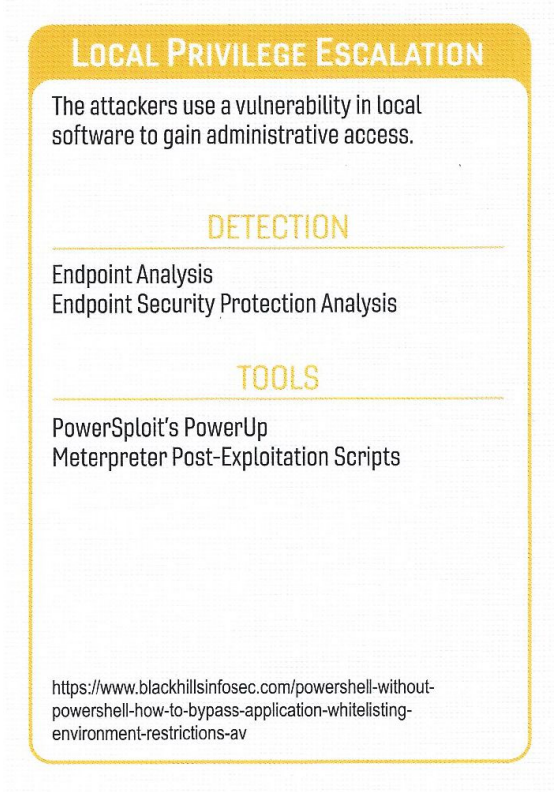
Types of cards

- 10 Initial compromise - First attack vector
- 8 Pivot and escalate - Foothold
- 8 Persistence - Maintain access
- 6 C2 & Exfiltration - Network channel
- 10 Inject - Adds randomness (good or evil)
- 10 Procedure - Helps with defense

Initial compromise



Pivot & escalate



Persistence

APPLICATION SHIMMING

The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Windows Assessment and Deployment Kit (ADK)

https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install

https://attack.mitre.org/techniques/T1138

C2 and exfil

HTTPS AS EXFIL

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINITY

https://www.metasploit.com

https://attack.mitre.org/techniques/T1032

https://github.com/byt3bl33d3r/SILENTTRINITY

Injects

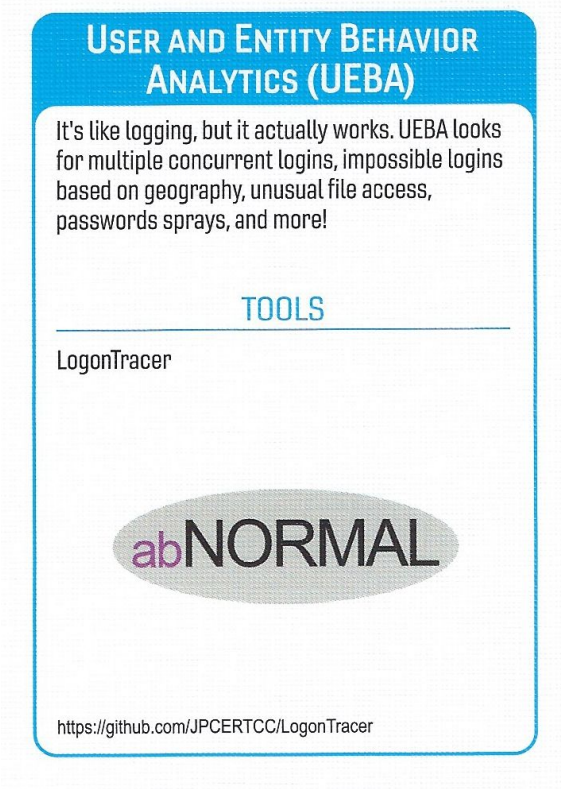
LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT

Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."

NOTES

They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!

Procedures


USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)
It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!
TOOLS
LogonTracer
abNORMAL
https://github.com/JPCERTCC/LogonTracer

Game start

- One person is the "Incident Master" (IM)
- IM picks one card from:
  - Initial compromise
  - Pivot & escalate
  - Persistence
  - C2 and exfil
- This builds "the incident"
- Players must identify each of these cards
  - Within 10 rounds

Before we start

- IM hands out Procedure cards
  - Usually this is 4 at random
- If all players from the same org
  - 4 that represent established protections
    - Documented policy identifying its use
    - Documented process to identify how its used
    - Audit trail to verify policy and process is followed
  - More than 4 cards at IM discretion
- Procedure cards give +3 to dice roll

Game play

- Optional for non-tech players
  - Show all procedure cards
  - Helps to identify what they can try
  - Remaining cards do not generate a +3 bonus
- IM identifies initial symptom
  - CEO got a weird email
  - Disk space on a system is full
  - Internet is slow
- Symptom not necessarily security related

Round one!

- Players discuss to identify what to do first
- One player rolls the dice
- Procedure matching attempt? If so +3
- Score of:
  - 1-10 = Attempt failed
  - 11-20 = Attempt successful
  - 1 or 20 = add inject card

IM's response

- If roll failed, round is done
  - 3 failed rounds in a row adds inject card
- If roll successful, players get a clue
  - Usually this means one card is revealed
  - Card depends on what they were targeting
- Move to next round
  - 10 rounds or incident fails

IM should track

- What procedure is played each round
  - Wait 3X rounds per procedure
- Success/failure of each round
  - 3X failed in a row gains an inject card
- Number of rounds played
  - 10 rounds or its a failure

Round	Procedure	S/F
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Special combos

DATA UPLOADED TO PASTEBIN

Bummer, the attackers have posted internal sensitive data on Pastebin. Your customers are now informed of the attack by the media.

NOTES

It happens... a lot, but it's just pure evil. Time to bring in Upper Management and the Legal Team.

CRISIS MANAGEMENT

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

For more info

https://www.backdoorsandbreaches.com